CONNECTED COMMUNITIES PROCUREMENT and IMPLEMENTATION GUIDANCE

QUESTIONS TO ASK INTERNALLY

SLTT governments are increasingly pursuing cost savings and operational efficiency by adopting Internet connected technology solutions. Integrating these technologies—including Internet of Things, Artificial Intelligence, 5G, and cloud computing—in connected communities offers the potential for enhanced and sustainable services to citizens. However, it also brings about new risks to critical infrastructure and the potential compromise of the security of sensitive government and personal data.

State, Local, Tribal, and Territorial (SLTT) officials can utilize these questions to clarify their goals and assess potential vendors' alignment with existing data protection and privacy as well as operational risk management.

PURPOSE AND OBJECTIVES:

- Q: What is the desired outcome this system will achieve? What is the problem you are solving?
- Q: How does this solution improve your community?
- Q: What are the social impacts of implementing this solution?

OPERATIONAL RISK MANAGEMENT:

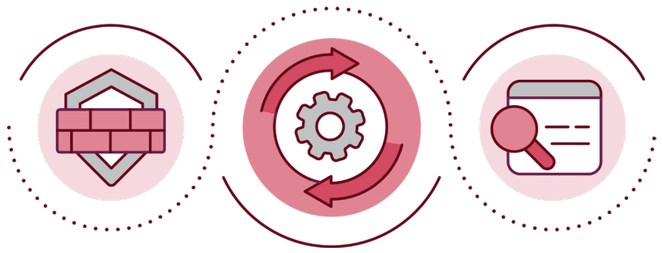
- Q: Can this solution continue to operate if the vendor goes out of business or if you decide to no longer work with the vendor?
- Q: What risks does this solution introduce into your community that were not present before or what existing risks does this solution amplify?
- Q: How would failure of the technology or a security incident impact your community?
    - Is the technology implemented in critical infrastructure?
    - Is your community equipped to manage the loss of the system or multiple assets?
    - Is your community equipped to manage the security fallout from the incident?
- Q: Are there manual backups in place in case of a technology failure? If so, is the manual backup automatically engaged upon system failure?
    - In the circumstance of a wider negative impact to physical systems (risk of injury/loss of life or otherwise negative impact), do you have a plan in place to communicate and coordinate with the public, first responders, and other government officials?
- Q: Are you able to reasonably manage the consequences, understand the technologies and systems sufficiently to assign responsibility, and take steps to mitigate such negative impacts?

DATA PROTECTION AND PRIVACY:

- Q: Will the vendor provide training to your organization's staff on how to manage and secure the data generated by the smart city technologies?
- Q: What kind of ongoing support will be available?
- Q: What role will your organization have in managing and securing the data generated by the smart city technologies, and how will this be defined in the contract with the vendor?
- Q: How will the vendor ensure that any third-party contractors or partners who have access to the data also comply with data protection requirements?
- Q: How will you audit the vendor's data protection practices and ensure ongoing compliance throughout the contract period?
- Q: Do you have a copy of all the data that this technology collects?

INTEROPERABILITY:

- Q: Do your products and platforms offer built-in integration support, such as application programming interfaces (API), for other common connected devices and software?
- Q: Will the vendor provide support services such as product testing and product integrations as part of the installation process?
- Q: Does the vendor have ongoing partnerships with other Internet of Things (IoT) and connected device vendors?
- Q: Does the product use the most common and/or open IoT protocols and standards, or are protocols used by the device proprietary?



CISA has multiple resources available to support SLTT partners including: (1) ICT Supply Chain Risk Management Task Force Resources, (2) voluntary cross-sector Cybersecurity Performance Goals (CPGs), (3) Risk Considerations For Managed Service Provider Customers, and (4) State And Local Cybersecurity Grant Program (SLCGP).